commutation de niveau 2

motivations

- relier plusieurs réseaux locaux
- Pourquoi plusieurs réseaux locaux ?

- pour relier des réseaux locaux internes qui se sont développés indépendamment, éventuellement avec des technologies différentes. Ex.: un réseau local par service de l'entreprise, développé par chaque service sans en référer aux voisins ni au central.
- pour des raisons d'éloignement géographique: liaison laser pour relier les réseaux locaux de 2 bâtiments
- pour mieux répartir la charge. Ex.: faire en sorte que le trafic interne d'un LAN reste sur le LAN et ne polue ni les autres LAN ni le réseau fédérateur (backbone).
- pour palier les limitations des LAN en matière de longueur de cable
- pour éviter qu'un équipement défectueux puisse écrouler l'ensemble de l'entreprise
- pour des raisons de sécurité

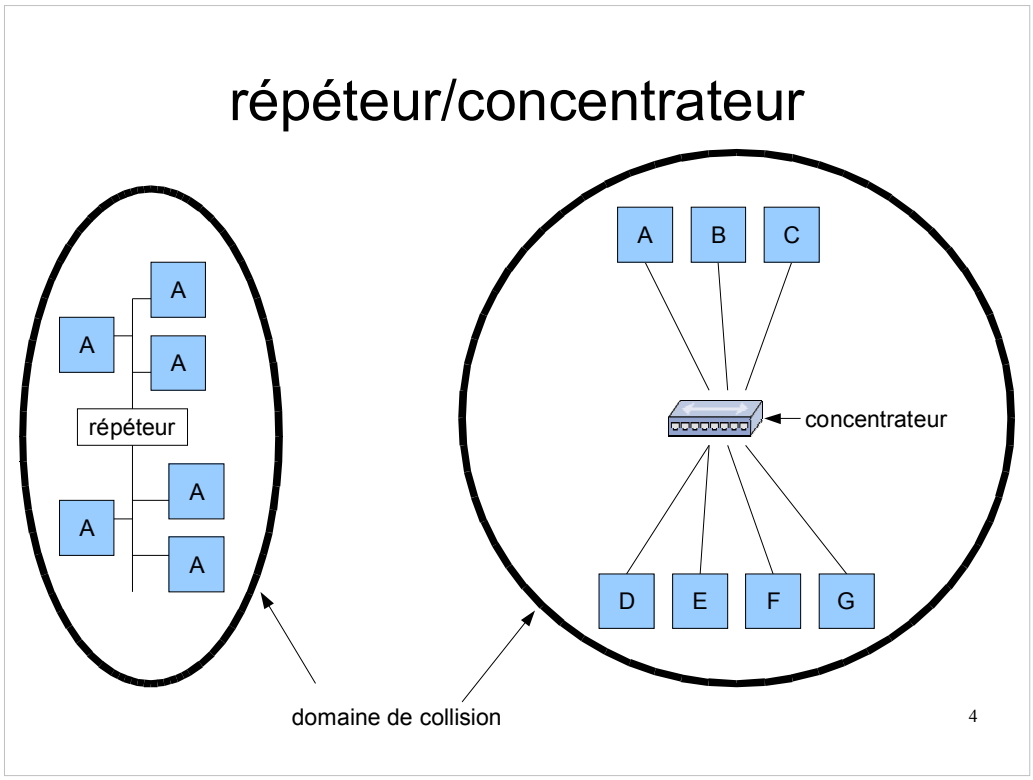
Ce sont des matériels différents qui peuvent répondre à ces motivations.

matériel de commutation

- répéteur
- concentrateur (hub)
- pont (bridge)
- commutateur (switch)
- routeur
- passerelle

Couche	matériel
Application	passerelle d'application (mandataire (proxy)
transport	passerelle de transport
réseau	routeur
liaison de données	pont/commutateur
physique	répéteur/concentrateur

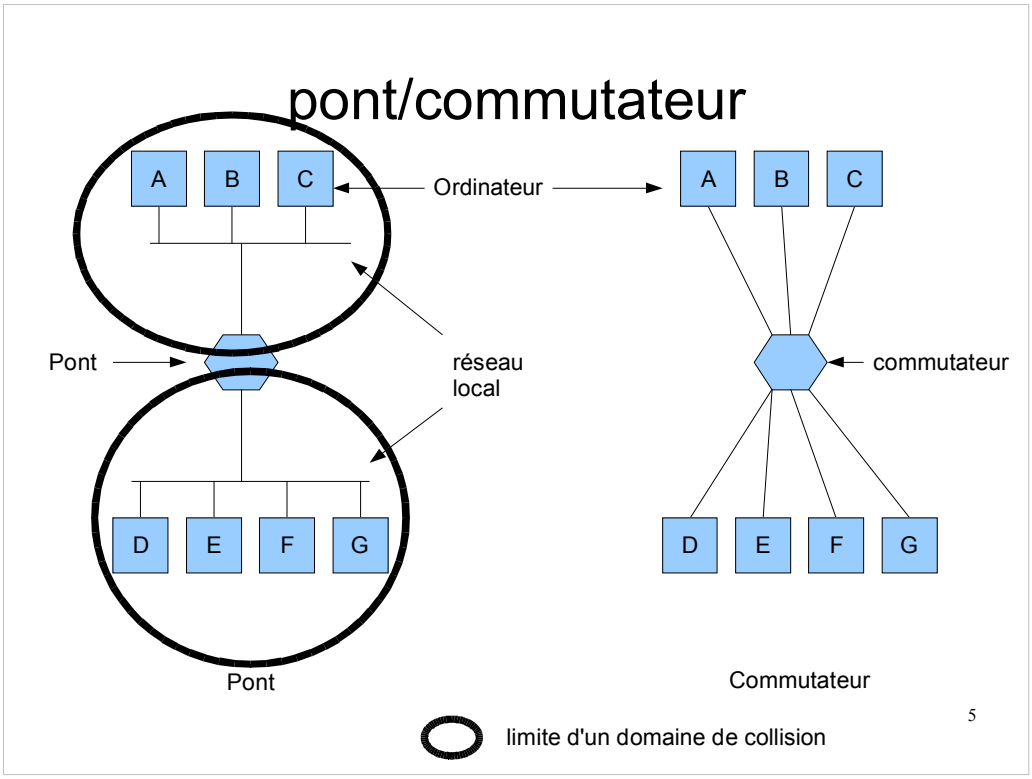
- Ces équipements n'opérent pas tous au même nivreau. La couche au niveau de laquelle ils opèrent détermine les informations auxquelles ils ont accès/qu'ils peuvent modifier.
- répéteur: concentrateur: rediffuse les paquets reçus sur une interface vers l'autre (ou les autres) après une éventuelle amplification du signal. Tout est retransmis
- Pont: relie deux segments ethernet et tente de ne laisser passer que les trames qui ont vocation à passer d'un segment à un autre. Les échanges entre machines d'un même segment ne sont ainsi pas censés passer le pont. Le pont délimite des domaines de collisions
- commutateur: un pont reliant plusieurs segment etthernet
- routeur: élément reliant plusieurs réseaux IP différents
- passerelle: éléments reliant plusieurs réseaux de technologies différentes. De nos jours, en langage courant, le terme passerelle a tendance à être utilisé comme synonyme de routeur.



- répéteur: agit au niveau physique et connecte deux cables pour en simuler un plus grand. Ethernet 10Mb/s: 4 répéteurs pour atteindre une taile maxi de 2500m. Un répéteur amplifie en général le signal.
- concentrateur (hub): opére au niveau physique. Relie entre elles leurs diversent entrées. Pas d'amplification du signal. Les signaux reçus sur une entrée sont répercutés sur les autres entrées.

Les réseaux reliés à un répéteur ou à un concentrateur forment un ensemble de collisions global.

D**omaine de collision** : ensemble des hôtes réseau dont les émissions peuvent provoquer une collision les unes avec les autres.



un pont t un commutateur achemine/filtre le trafic en examinant les adresses des trames.

chaque ligne d'un pont ou d'un commutateur représente un domaine de collision distinct. Exemple: lorsque l'ordinateur A envoie une trame à l'ordinateur B, le pont rejette la trame car il sait que B est du même côté que la trame. Il ne peut donc y avoir collision entre des trames internes au Lan1 et des trames internes au LAN2.

On confond souvent pont et commutateurs. Traditionnellement, un pont peut servir à relier des Lan de types différents (WiF/Ethernet par ex.) tandis qu'un commutateur a toutes ses lignes du même type.

De nos jours, le lien entre le commutateur et l'élément réseau (ordinateur, ...) qui est relié à l'un de ses ports se fait en full duplex. Dans ce cas, CSMA/CD n'est pas utilisé. Il est remplacé par un simple contrôle de flux.

Le fait d'avoir un domaine de collision par port fait que les commutateurs ne perdent jamais de trames à cause de collisions. Par contre, si une machine émet plus rapidement que le commutateur peut écouler les données, une fois que la mémoire tampon du port correspondant sera pleine, les trames qu'il ne peut traiter seront supprimées.

Un pont/commutateur augmente donc les performances du réseau en découpant un domaine de collision unique en plusieurs domaines de collisions, voire en supprimant les domaines de collision (full-duplex avec un commutateur).

Un pont ou un commutateur permet aussi d'améliorer la sécurité du réseau en filtrant les trames : un poste pirate ne verra pas le trafic qui ne lui est pas destiné. En pratique, des attaques sur les tables d'adresses Mac des commutateurs existent.

routeur/passerelles

- routeur: s'appuie sur l'adresse de la couche réseau (par ex. adresse IP) pour choisir la ligne de sortie du paquet
- passerelle de transport: protocoles de transports différents (tcp/ip <-> ATM)
- passerelle applicative: transformation du format des données (ex.: internet -> SMS)

méthode d'apprentissage des ponts/commutateurs

- algo de transmission d'une trame provenant d'un LAN A
  - si la trame est à destination de A, on la rejette
  - si la trame est à destination d'un autre LAN connu, on le transmet sur le port derrière lequel se trouve le LAN
  - si la trame est à destination d'un LAN inconnu, on la diffuse sur tous les ports (innondation)
- apprentissage (backware learning)
  - on retient les ports des adresses sources des trames que l'on voit passer
  - au bout d'un certain temps (en secondes) sans voir passer de trames avec l'adresse d'un hôte donné, on efface l'hôte des tables

redondance et arbre de recouvrement

- résistance au panne = redondance
- la redondance est impossible avec ethernet: les paquets bouclent
- Solution: algo « spanning tree » pour désactiver les ports faisant des boucles: on ne laisse actifs que les ports correspondant à un lien d'un arbre couvrant (arbre => pas de boucle)
- 802.1D-1998: spanning tree
- 802.1D-2004: rapid spanning tree

réseaux virtuels (VLAN)

- définition
- intérêt

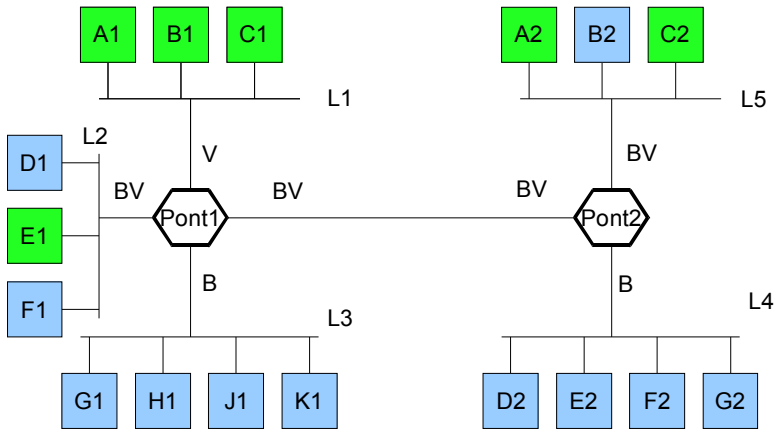
il est parfois utile que des machines physiquement proches soient sur des réseaux différents. Les raisons peuvent être liées à la sécurité, d'autres pour des raisons de charge du réseau que l'on souhaite répartir sur plusieurs réseaux.

D'un point de vue cablage, cela supposerait que ces machines proches physiquement soient reliées (brassées) sur des matériels actifs (concentrateurs, commutateurs) différents.

Gérer un tel réseau est très complexe. A chaque déménagement, il faut prévoir un matériel actif ad hoc dans le local de brassage auquel est relié la prise du poste et y brasser le bon cable. C'est une charge lourde.

Les VLANs permettent de faire cela au niveau logiciel et de découper un commutateur ethernet en commutateurs virtuels identifiés par un identifiant de VLAN.

VLAN: exemples



10

on définit des VLANs sur les ponts et on y affecte les postes. Les postes sont regroupés en LAN sur concentrateurs ou 10base2 ou 10Base5 (aucune différence entre ces trois cas d'un point de vue logique)

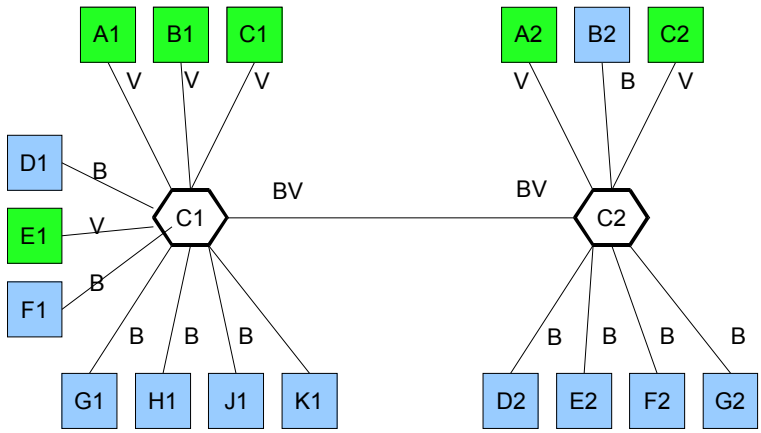
Les trames qui seront envoyées sur chaque LAN seront vues de toutes les machines du LAN car les postes d'un LAN sont reliées à l'aide d'un concentrateur.

Exemples:

- trame unicast de G1 vers D2: sur L3 puis Pont 1 puis Pojt2 puis L4/D2. Les ponts jouent leur rôle (apprentissage des adresses mac)
- trame unicast de A1 vers A2: A1/L1/Pont1/Pont2/L5/A2. La trame a été transmise sur L5 et donc B2 a pu la voir passer (si en mode promiscuous)
- trame de diffusion de D1 sera diffuée sur L2, L3 (bleu), L4 et L5 mais pas sur L1.

Problème; comment identifier le VLAN de trames qui circulent entre Pont1 et Pont2 ?

VLAN: exemples



11

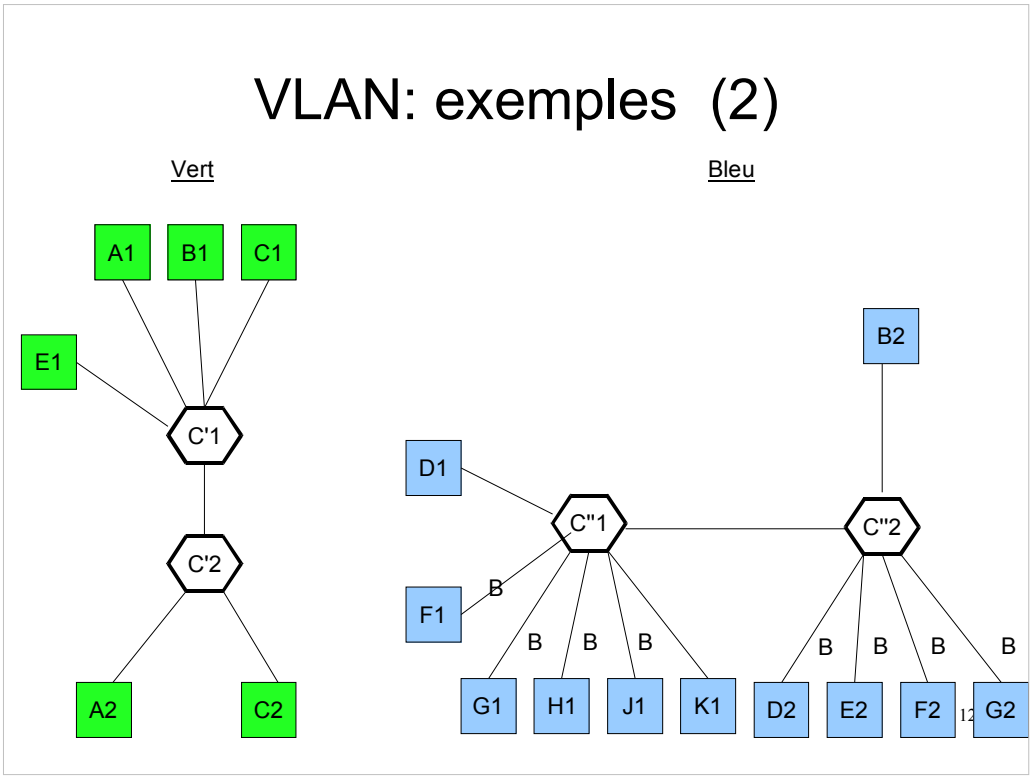
Avec des commutateurs, les choses sont plus claires :

- seuls les ports des liens entre commutateurs sont communs à plusieurs VLAN
- les ports sur lesquels sont les postes sont sur un seul VLAN

On évite ainsi que des paquets destinés de l'un des VLAN soit transmis et vus par des postes appartenant à d'autres VLAN.

Exemples:

- trame unicast de G1 vers D2: C1 -> C2 -> D2
- Problème; comment identifier le VLAN de trames qui circulent entre C1 et C2 ?



Avec des commutateurs, les choses sont plus claires :

- les VLAN permettent de découper les commutateurs en autant de sous-commutateurs virtuels indépendant qu'il y a de VLAN
- Le réseau précédent est équivalent au réseau ci-dessus à un détail près: le lien entre les deux commutateurs est utilisé par les deux VLAN :
  - chaque VLAN n'a donc pas tout le débit à sa dispositoin contrairement à ce que laisse penser le schéma ci-dessus
  - il faut pouvoir identifier à quel VLAN appartient une trame qui circule sur ce lien inter-commutateur: norme IEEE 801.1Q

VLAN: détermination

- affectation d'un ou plusieurs (IEEE 802.1Q) VLAN à chaque port d'un commutateur/pont
- affectation d'adresse MAC à un VLAN
- via des informations des couches supérieures (adresse IP par ex.)

Comment un commutateur détermine-t-il à quel VLAN appartient à un paquet ? Une solution consiste à affecter un VLAN à chaque port du commutateur. 3 méthodes sont traditionnellement utilisées pour ça :

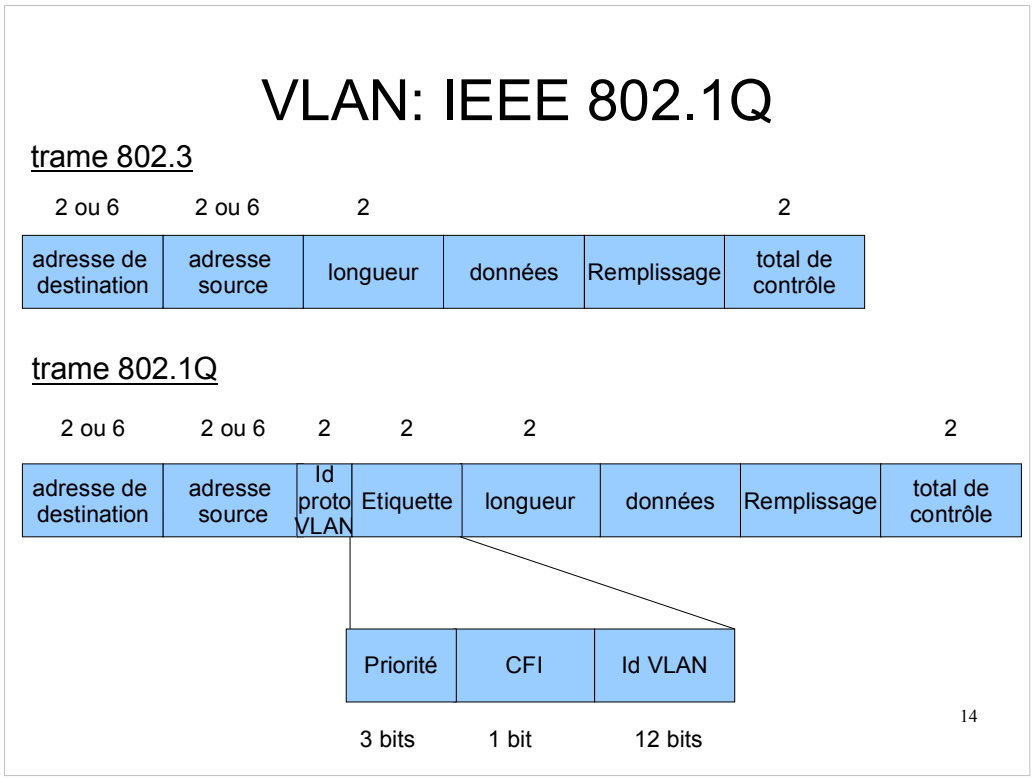
- affecter le vlan par port en configurant statiquement le commutateur
- affecter le VLAN en fonction de l'adresse MAC source du paquet
- affecter le VLAN en fonction du sous-réseau auquel appartient l'ip source du paquet (pour IP)
- affecter le VLAN en fonction des données retournées par un serveur d'authentification suite à l'authentification du poste relié au port du commutateur (802.1X)

La première et la quatrième solution sont souvent utilisées.

Ces méthodes ne règlent pas tous les problèmes et notamment la façon de gérer des ports, des liens sur lesquels des paquets appartenant à plusieurs VLAN peuvent circuler.

Une solution efficace consisterait à indiquer le VLAN directement dans l'entête du paquet.

Pb: il n'y a pas la place pour le faire dans une entête 802.3.



un VLAN est associé à chaque trame. Pour rendre possible la détermination de ce VLAN dans tous les cas, accèlérer le traitement, on peut imaginer d'ajouter un identifiant de VLAN à chaque trame. C'est ce que propose la norme IEEE 802.1Q.

Cela pose un gros problème de compatibilité avec le matériel existant. En pratique, ces champs supplémentaire est réellement utile entre matériel actif. Voici comment se passent les choses en pratiques :

- à chaque port de commutateur auquel est relié une station de travail.
- un paquet venant d'une station est non étiqueté mais il le sera par le commutateur;
- les ports servant aux communication entre commutateurs sont déclarés comme étiquetés (Tagged): les trames qui y transitent sont à la norme 802.1Q
- un paquet à destination d'un station de travail sera détaggé (remis à la norme 802.3) par le commutateur auquel est relié la station.

L'identification du format se fait grace au champ « Id de protocole VLAN » qui a une valeur de 0x8100 (>1500 donc ça ne peut pas être une longueur)

une étiquette contient l'id du VLAN de la trame (sur 12 bits)

un champ de 3 bits identifie la priorité de la trame (sans rapport avec les VLAN mais ajouté à la norme)

un champ d'un bit « Canonical format indicator » indique si le champ de données contient une trame 802.5 destinée à un LAN 802.5.

ces deux champs n'ont rien à voir avec les VLAN (politique des comités de normalisation)